Exploration of topologies of coupled nonlinear maps (Chaos theory)

René Lozi

Published in proceedings of *MENDEL 2015, 21st International Conference on Soft Computing*, Mendel Series Volume 2015, June 23-25, Brno, Czech Republic, Matousek Radek Ed. ISSN 1803-3814, pp. 223-236

EXPLORATION OF TOPOLOGIES OF COUPLED NONLINEAR MAPS (CHAOS THEORY)

René Lozi

University of Nice-Sophia Antipolis
Laboratory J.A. Dieudonné, UMR CNRS 7351
Parc Valrose, 06108 NICE Cedex 02
France
rlozi@unice.fr

Abstract: *We explore several topologies of network of 1-D coupled chaotic mapping (mainly tent map and logistic map) in order to obtain good Chaotic Pseudo Random Number Generators (CPRNG). We focus first on two-dimensional networks. Two coupled maps are studied:* TTL^{RC} *non-alternative, and* TTL^{SC} *alternative. In this case, those networks are equivalent to 2-D maps which achieve excellent random properties and uniform density in the phase plane, thus guaranteeing maximum security when used for chaos based cryptography.*
Moreover an extra new nonlinear CPRNG: $MTTL_2^{SC}$ *is proposed. In addition, we explore higher dimension and the proposed ring coupling with injection mechanism enables us to achieve the strongest security requirements.*

Keywords: *chaos, mappings, chaotic pseudo-random numbers, attractors.*

1 Introduction

The tremendous development of new IT technologies, e-banking, e-purchasing, Internet of Things, etc. nowadays increases incessantly the needs for new and more secure cryptosystems. They are used for information encryption, pushing forward the demand for more efficient and secure pseudo-random number generators [1] in the scope of chaos based cryptography. Indeed, chaotic maps show up as perfect candidates, able to generate independent and secure pseudo-random sequences (used as information carriers or directly involved in the process of encryption/decryption). However, the majority of well-known chaotic maps are not naturally suitable for encryption [2] and most of them do not exhibit even satisfactory properties for encryption. To deal with this open problem, we propose the new idea to couple tent and logistic map, and to add a specific injection mechanism to capture the escaping orbits. Good results are demonstrated with two different kinds of coupling, simple and ring-coupling in dimension 2, thus increasing the complexity of the system. However as those results are not completely satisfactory, by exploring further topologies of coupled nonlinear maps, we propose an improved geometry of coupling which allows us to describe a new 2-D Chaotic Pseudo Random Number Generator (CPRNG).
The various choices of the PRNG and crypto algorithms are nowadays necessary to provide continuous, reliable security system. We use here a software approach because it is easy to change cryptosystem to support protection, whereas hardware requires more time and big expenses. For instance, after the secure software application called Wi-Fi Protected Access (WPA) protocol has been broken, it was simply updated and no expensive hardware needed to be bought.
Consequently, it is necessary to have an alternative way of secure information transmission. Chaos based methods are very promising for application in information security [3, 4]. One of the evidences is, that needs for data protection are increased and that encryption procedures requires generating pseudo-random sequences with very long periods. The chaotic maps when used in sterling way could generate not only chaotic number but also pseudo-random numbers as we will show here.
Here we represent an original idea combining of tent and logistic maps for new chaotic PRNG design. Since, it is a very responsible and challenging task to design CPRNG applicable to cryptography, numerous analysis have been fulfilled. Essentially we focus on 2-D map as a more difficult task achieving excellent chaotic and randomness properties. The 3-steps injection mechanism, ring- and auto-coupling techniques are used to achieve complex and uniform dynamics. We demonstrate excellently puzzled chaotic dynamics in the space exhibiting sufficient randomness properties only for 2-D map. The most significant tests were successfully passed. Moreover, higher dimensional systems are here proposed as well, they provide also good candidates for CPRNG.

In Sect. 2 we recall briefly the dawn and the maturity of chaos research. In Sect. 3 we explore topologies of network of coupled chaotic maps. In Sect. 4 we propose a new higher-dimensional map, before concluding is Sect. 5.

2 The dawn and the maturity of chaos research

The study of nonlinear dynamics is relatively recent with respect to the long historical development of the early mathematics since the Egyptian and the Greek civilization, even if one includes in this field of research the pioneer independent works of Julia [5] and Fatou [6] related to one-dimensional maps with a complex variable, near a century ago.

Sharkovsky's order was found in 1962 [7], albeit published in 1964. In France I. Gumosky and C. Mira began their mathematical researches in 1958 [8], they developed very complicated studies of iterations. One of the best known formulas they published is:

$$\begin{cases} x_{n+1} = f(x_n) + by_n, \\ y_{n+1} = f(x_{n+1}) - x_n, \end{cases} \quad with \quad f(x) = ax + 2(1-a)\frac{x^2}{1+x^2}, \tag{1}$$

which can be considered as a non-autonomous mapping from the plane $\mathbf{R}^2$ into $\mathbf{R}^2$ exhibiting aesthetic chaos (Figs. 1, 2). Slights change in the parameter value leads to very different shapes.

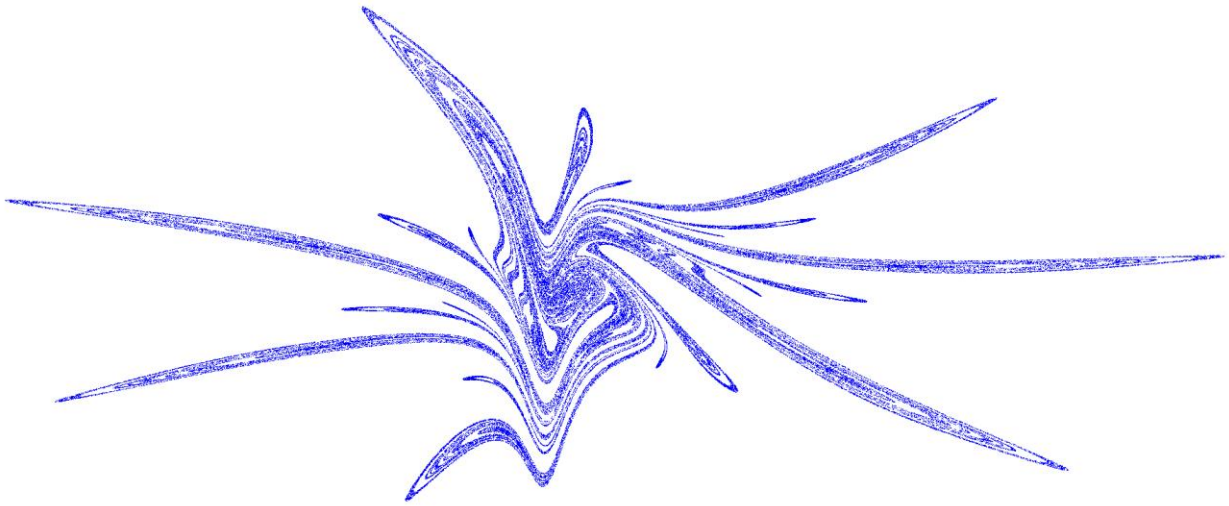


Figure 1: Gumowsky-Mira attractor for the parameter value: a = -0.918, b = 0.9 .

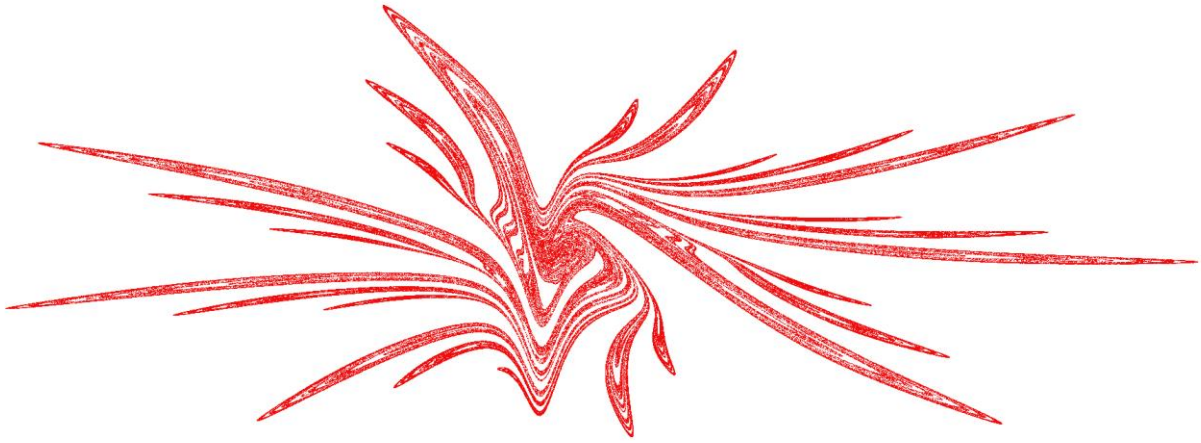


Figure 2: the same attractor for the parameter value: a = -0.93333, b = 0.92768.

In Japan the Hayashi' School (with disciples like Ikeda, Ueda and Kawakami) few years before were motivated by applications to electric and electronic circuits. The Ikeda attractor

$$\begin{cases} x_{n+1} = 1 + u(x_n \, cost_n - y_n \, sint_n), \\ y_{n+1} = u(x_n \, sint_n + y_n \, cost_n), \end{cases} \quad with \quad t_n = 0.4 - \frac{6}{1 + x_n^{\,2} + y_n^{\,2}}, \tag{2}$$

has a chaotic attractor for $u \geq 0.6$ [9] (Fig. 3).

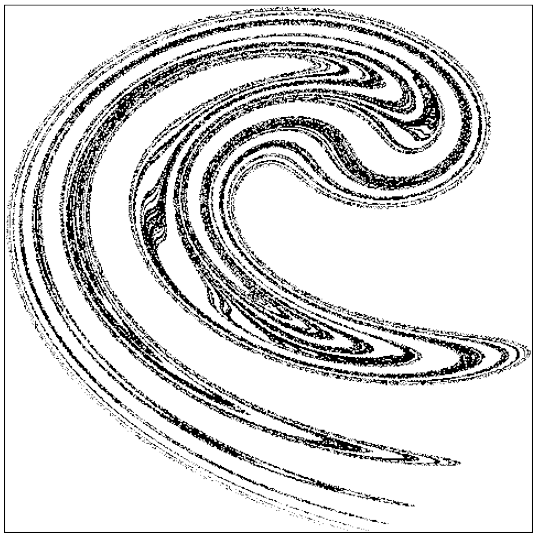


Figure 3: Ikeda attractor (from [9])

In 1983 Chua invented his famous electronic circuit [10] exhibiting a chaotic strange attractor on oscilloscope screen. Since then, thousand of papers have been published on this general topic; however the main trend of mathematics is slowness, because any progress is based on rigorous proof. Numerous problems are still unsolved such as the simple one: does Hénon map [11] possess a strange attractor rigorously proved?
Nevertheless, in spite of this lack of rigorous mathematical results, nowadays engineers are actively working on application of chaos for several purposes: global optimization, genetic algorithms, CPRNG (Chaotic Pseudo Random Number Generators), cryptography, etc. They use non linear maps for practical applications without the need of sophisticated theorems.

Dynamical systems which present mixing behavior and that are highly sensitive to initial conditions are called chaotic. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems This effect popularly known as the as the butterfly effect, renders long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. Mastering the global properties of those dynamical systems is today a challenging issue we try to fix exploring several topologies of network of coupled maps.

3 Exploring topologies of network of coupled chaotic maps

During the past Mendel 2014 conference, we have thoroughly described the most known 1-D and 2-D dynamical systems [12]. In this section we consider only two 1-D maps: the logistic map

$$f_\mu(x) \equiv L_\mu(x) = 1 - \mu x^2 \tag{3}$$

associated to the dynamical system

$$x_{n+1} = f_\mu(x_n) \tag{4}$$

and the symmetric tent map

$$f_\mu(x) \equiv T_\mu(x) = 1 - \mu |x| \tag{5}$$

In both cases, μ is a control parameter that has impact to chaotic degree, and both mappings are sending the one-dimensional interval [-1, 1] into itself.
Those two maps have also been fully explored in the hope of generating pseudorandom number easily [13]. However the collapsing of iterates of dynamical systems or at least the existence of very short periodic orbits, their non constant invariant measure, and the easily recognized shape of the function in the phase should space, should lead to avoid the use of such one-dimensional map (logistic, baker, or tent, etc.) or two dimensional map (Hénon, standard or Belykh, etc.) as a pseudo-random number generator (see [14] for a survey). However, the very simple implementation in computer program of chaotic dynamical systems led some authors to use it as a base of cryptosystem [15, 16]. They are topologically conjugate, that means they have similar topological properties (distribution, chaoticity, etc.) however due to the structure of numbers in computer realization their numerical behavior differs drastically. Therefore the original idea here is to combine features of tent (T_μ) and logistic (L_μ) maps to achieve new map with improved properties, trough combination in several topologies of network. An extended study of Sec. 3 can be found in [17].
Looking to both equations (3) and (5) we can inverse the shape of the graph of the tent map *T* on the step of logistic map *L*. Thus, our proposition has the form

$$f_\mu(x) \equiv TL_\mu(x) = \mu|x| - \mu x^2 = \mu(|x| - x^2) \tag{6}$$

Recall that both logistic and tent maps are never used in cryptography because they have weak security (collapsing effect) [18, 19] if applied alone. Thus, systems are often used in modified form to construct CPRNG [20, 21]. The system [22] (Lozi & al.) provides method to increase randomness properties of the tent map over its coupling.

Nevertheless in another way, we propose to couple T_μ map over combination with TL_μ map (6). When used in more than one dimension, TL_μ map can be considered as a two variable map

$$TL_\mu(x^{(1)}, x^{(2)}) = \mu(|x^{(1)}| - (x^{(2)})^2) \tag{7}$$

Hence it possible to define a mapping $M_p : J^p \to J^p$ where $J^p = [-1,1]^p \subset \mathbf{R}^p$

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{pmatrix} T_\mu(x_n^{(1)}) + TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ \vdots \\ T_\mu(x_n^{(p)}) + TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{pmatrix} \tag{8}$$

Note that, the system dynamics is unstable and trajectories quickly spread out. Therefore, to solve the problem of holding dynamics in the torus $J^p = [-1,1]^p \subset \mathbf{R}^p$ the following injection mechanism has to be used:

$$\begin{cases} if\,(x_{n+1}^{(i)} < -1) \quad then \quad add \quad 2 \\ if\,(x_{n+1}^{(i)} > 1) \quad then \quad substract \quad 2 \end{cases} \tag{9}$$

hence for $1 \le i \le p$, points come back from $[-3,3]^p$ to $[-1,1]^p$.
Used in conjunction with T_μ the TL_μ function allows to establish mutual influence between system states. The function is attractive because it performs contraction and stretching distance between states improving chaotic distribution. Thus, the TL_μ function is a powerful tool to change dynamics.
The coupling of the simple states has excellent effect on chaos achieving, because:

- Simple states interact with global system dynamics, being a part of it.
- The states interaction has the global effect.

Hence, if we use TL_μ to make impact on dynamics of the simple maps then excellent effect on chaoticity and randomness could be achieved. The proposed function improves complexity of a simple map. In order to study the received system we use a graphical approach, however other theoretical assessing functions are also involved.

Published in proceedings of *MENDEL 2015, 21st International Conference on Soft Computing*, Mendel Series Volume 2015, June 23-25, Brno, Czech Republic, Matousek Radek Ed. ISSN 1803-3814, pp. 223-236

Note that the system (8) can be seen in the scope of a general point of view, introducing constants k^i which generalize considered topologies. It is called alternative if $k^i = -1^i$ or $k^i = -1^{i+1}$, $1 \le i \le p$, or non-alternative if $k^i = +1$, $1 \le i \le p$; or $k^i = -1$, $1 \le i \le p$. It can be a mix of alternative and non-alternative if $k^i = +1$ or -1 randomly.

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{pmatrix} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + k^2 \times TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ \vdots \\ T_\mu(x_n^{(p)}) + k^p \times TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{pmatrix} \tag{10}$$

3.1 2-D topologies

The initial purpose of new CPRNG design was to obtain excellent uniform distribution, successfully passing randomness and chaoticity tests. Thus we propose to consider firstly two 2-D models: alternative ($k^1 = -1$; $k^2 = 1$) and non-alternative ($k^1 = k^2 = 1$). However, coupling between states by TL_μ can be made in different ways:

- Ring coupling with two choices

$$TL_\mu^{RC}(x^{(1)}, x^{(2)}) = \begin{cases} T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \\ T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \end{cases} \tag{11}$$

or

$$TL_\mu^{RC}(x^{(2)}, x^{(1)}) = \begin{cases} T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \\ T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \end{cases} \tag{12}$$

- Simple coupling with also two choices

$$TL_\mu^{SC}(x^{(1)}, x^{(2)}) = \begin{cases} T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \\ T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \end{cases} \tag{13}$$

or

$$TL_\mu^{SC}(x^{(2)}, x^{(1)}) = \begin{cases} T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \\ T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \end{cases} \tag{14}$$

The general form of the new 2-D map we consider is as follow:

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu(x_n^{(i)}, x_n^{(j)}) \\ T_\mu(x^{(2)}) + k^2 \times TL_\mu(x_n^{(i')}, x_n^{(j')}) \end{cases} \tag{15}$$

with *i, j; i', j' = 1* or *2* and TL_μ being either TL_μ^{RC} or TL_μ^{SC}.

Remark: Ring-coupling can be expected to higher dimension but not the single case because we obtain the same expression of the function. However, it is undesirable to use $TL_\mu^{SC}(x^{(1)}, x^{(2)})$ because (13) gives the trivial result:

$$M_p\begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1(T_\mu(x_n^{(1)}) - L_\mu(x_n^{(2)})) \\ T_\mu(x^{(2)}) + k^2(T_\mu(x_n^{(1)}) - L_\mu(x_n^{(2)})) \end{cases} = \begin{cases} k^1 \times L_\mu(x_n^{(2)}) \\ k^2 \times L_\mu(x_n^{(2)}) \end{cases}. \quad (16)$$

If one uses the $TL_\mu^{RC}(x^{(2)}, x^{(1)})$ alternative system then one of the states will have more "power" than another one, loosing good distribution of point property. For the same reason $TL_\mu^{SC}(x^{(1)}, x^{(2)})$ or $TL_\mu^{SC}(x^{(2)}, x^{(1)})$ non-alternative ($k = 1$) are not recommended to be used.

Therefore, we will consider only two 2-D systems: $TTL_\mu^{RC}(x_n^{(1)}, x_n^{(2)})$ **non-alternative**

$$TTL_\mu^{RC} = \begin{cases} x_{n+1}^{(1)} = 1 - \mu\left|x_n^{(1)}\right| + \mu(\left|x_n^{(2)}\right| - (x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1 - \mu\left|x_n^{(2)}\right| + \mu(\left|x_n^{(1)}\right| - (x_n^{(2)})^2) \end{cases} \quad (17)$$

and $TTL_\mu^{SC}(x_n^{(1)}, x_n^{(2)})$ **alternative**

$$TTL_\mu^{SC} = \begin{cases} x_{n+1}^{(1)} = 1 - \mu\left|x_n^{(1)}\right| - \mu(\left|x_n^{(1)}\right| - (x_n^{(2)})^2) \\ x_{n+1}^{(2)} = 1 - \mu\left|x_n^{(2)}\right| + \mu(\left|x_n^{(1)}\right| - (x_n^{(2)})^2) \end{cases} \quad (18)$$

Both systems were selected because they have balanced contraction and stretching process between states, allowing to achieve uniform distribution of the chaotic dynamics.

3.2 Randomness study of the new maps TTL_μ^{RC} and TTL_μ^{SC}

We are now assessing the randomness of both selected maps. The associated dynamical system is considered to be random and could be applied to cryptosystems if the chaotic generator meets the requirements 1-8 which are described on Fig. 4. If one of the criterions is not satisfied the behavior is less random than expected.

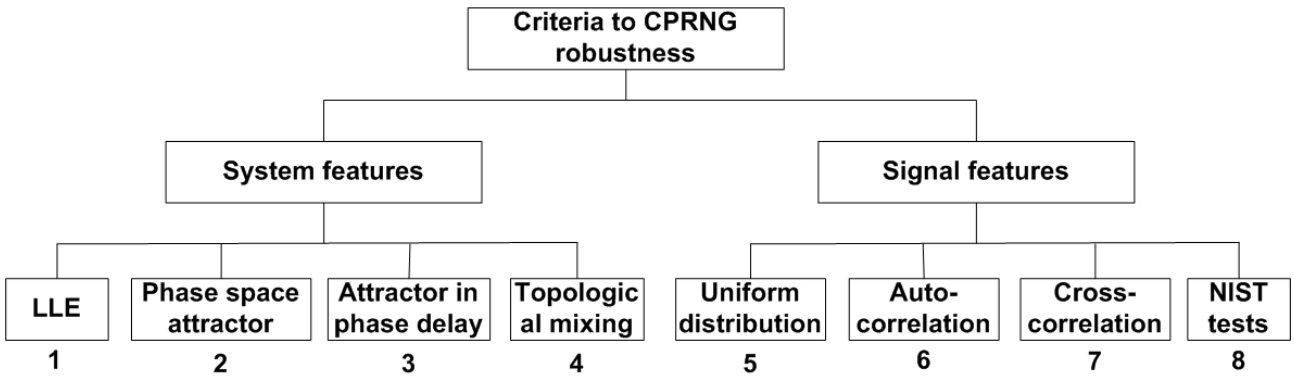
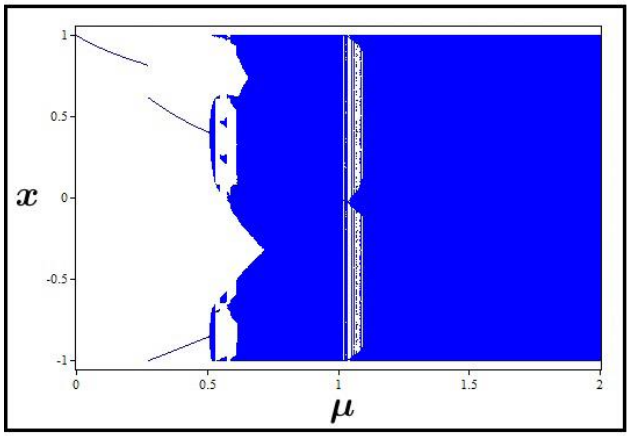


Figure 4: The main criteria for PRNG robustness (from [17])

Thus, to study the dependency to the parameter μ, a bifurcation diagram is drawn for which 9,000 points are plotted for each value of the parameter. The graphs look the same either for $x^{(1)}$ or $x^{(2)}$.



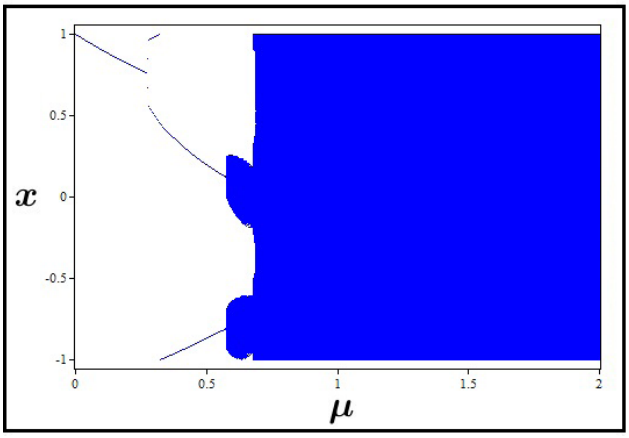
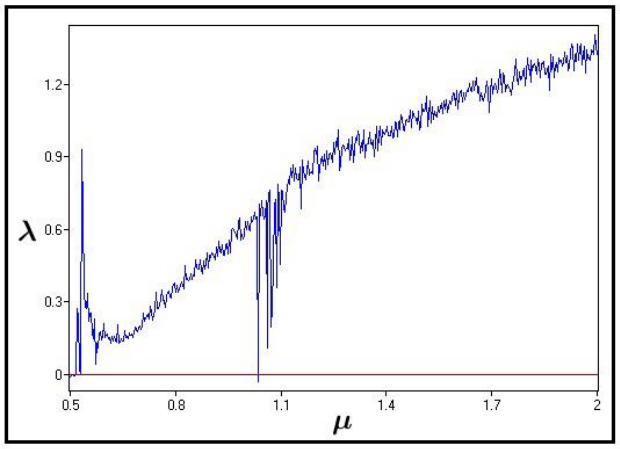


Figure 5 (left): Bifurcation diagram of 2-D new map TTL_{μ}^{RC} non alternative (17)

Figure 6 (right): Bifurcation diagram of 2-D new map TTL_{μ}^{SC} alternative (18)

For both graphs starting from $\mu = 0$ to $\mu = 0.25$, we can observe a period 1 (*i.e.* a fixed point). Then the steady-state response undergoes a so-called pitchfork bifurcation to period 2. Following bifurcation undergoes multiple periods. At higher μ values, the behavior is generally chaotic. However, for TTL_{μ}^{RC} near $\mu = 1.1$ periodic windows appear. The subsequent intervals show perfect chaotic dynamics.

A complementary study of chaos is the graph of the largest Lyapunov exponent which is a measure of the system sensitivity to initial conditions. When this exponent is strictly positive, the system exhibits chaotic behavior.



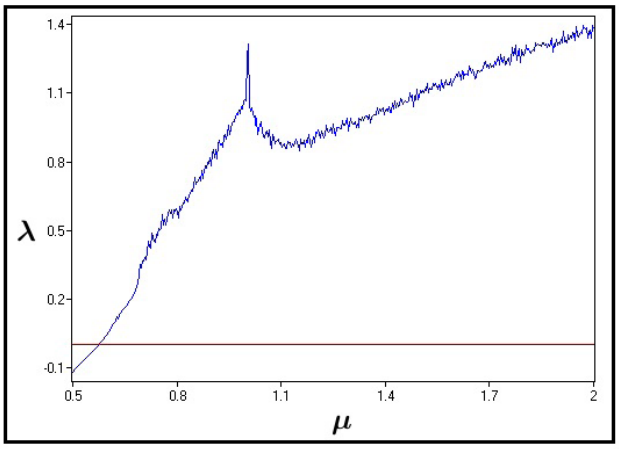
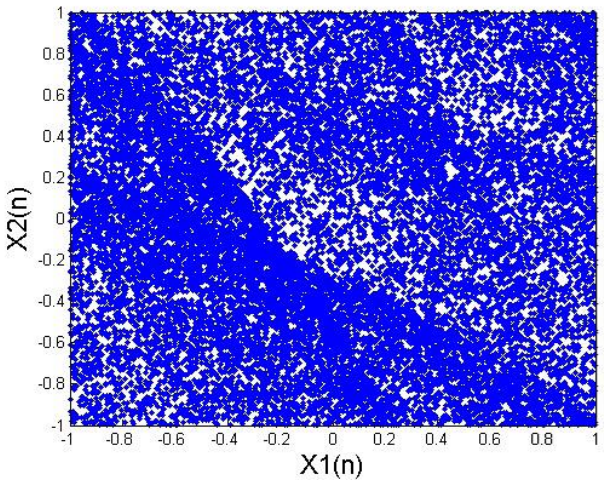


Figure 7 (left): Largest Lyapunov exponent of 2-D new map TTL_{μ}^{RC} non alternative (17)

Figure 8 (right): Largest Lyapunov exponent of 2-D new map TTL_{μ}^{SC} alternative (18)

Graphs of the Lyapunov exponent are in exact agreement with bifurcations ones, the strongest chaos arises at $\mu = 2$. Therefore we will continue our study fixing the parameter to this value. On the graphs for any given initial point x_0 trajectories look like chaotic. Hence, to be more accurate, we have to study the behaviour of iterated points in phase space and phase delay.



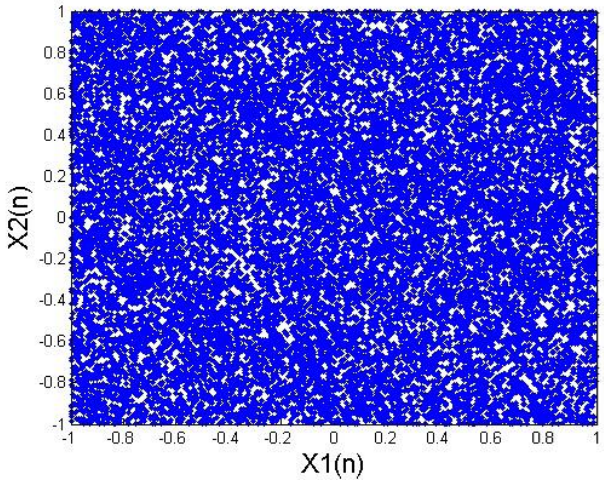
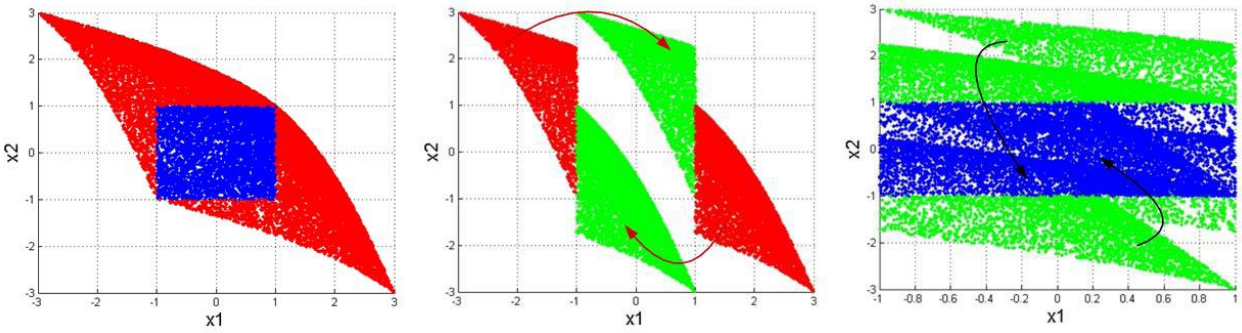


Figure 9 (left): Phase space behaviour of TTL_2^{RC} non alternative (17), plot of 20,000 points

Figure 10 (right): Phase space behaviour of TTL_2^{SC} alternative (18), plot of 20,000 points

To plot the attractor Figs. 9 and 10, 30,000 points have been generated, of which 10,000 points of the transient regime have been cut off.

The graphs of the attractor in phase space for TTL_μ^{RC} non alternative (Fig. 9) and TTL_μ^{SC} alternative (Fig. 10) maps are quite different. The first one has well scattered points on all the patterns, but there are some more "concentrated" regions forming curves on the graph. We will search understand why. Without the injection mechanism, points are scattered in the square $[-3,3]^2$ (Fig. 11a). Among the 20,000 generated points, 77 % are scattered out of the square $[-1,1]^2$. On the first step of injection mechanism (9), 69% points are injected to the rectangle $[-1,1]\times[-3,3]$ (Fig. 11b) after passing the second injection step (Fig. 11c) all points are driven base to the square $[-1,1]^2$ (Fig. 9). Therefore mechanism adds non-linearity and complexity to the system which is an advantage from the security point of view, in the case of cryptographic use.



(a) (b) (c)

Figure 11 (a): scattering of points by TTL_2^{RC}, plot of 20,000 points

Figure 11 (b): first step of injection mechanism (9)

Figure 11 (c): second step of injection mechanism (9)

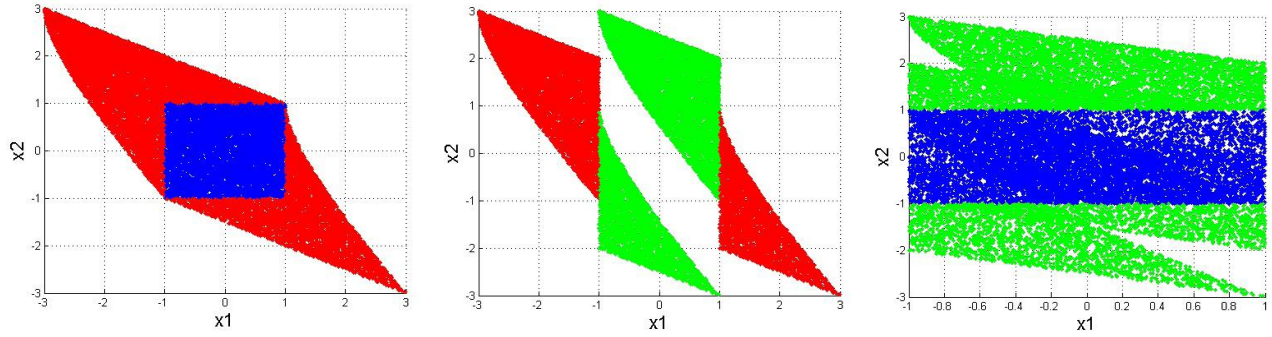


Figure 12 (a): scattering of points by TTL_2^{SC}, plot of 20,000 points

Figure 12 (b): first step of injection mechanism (9)

Figure 12 (c): second step of injection mechanism (9)

The graphs of the attractor in phase space for TTL_2^{SC} alternative map looks uniformly distributed on the square $[-1,1]^2$ without any visible concentrated regions (Fig. 10). The injection mechanism impact on the point distribution is given on the Fig. 12.

3.3 A new 2-D chaotic PRNG

Considering the results of section 3.2 it seems possible to improve the randomness of the 2-D topology. We observe that two regions (top-green and right-red) on the Fig. 12b could be pretty connected. First, let us rewrite the mapping TTL_μ^{SC} alternative (18) where $\mu = 2$ as follow:

$$TTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 4\left|x_n^{(1)}\right| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(\left|x_n^{(1)}\right| - \left|x_n^{(2)}\right|) \end{cases} \tag{19}$$

The first problem is that top green colored region occurs after injection is applied. Thus, we develop the system (19) in such way that green coloured region "stays" in such position without injection mechanism. Secondly, we need to reduce the width of the region. Evidently, it is possible to achieve this need by reducing the impact of the state x^1, with the new following map:

$$MTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 2\left|x_n^{(1)}\right| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(\left|x_n^{(1)}\right| - \left|x_n^{(2)}\right|) \end{cases} \tag{20}$$

and the injection mechanism (9) is used as well, but restricted to 3 phases:

$$\begin{cases} if\,(x_{n+1}^{(1)} > 1) \quad then \quad substract \quad 2 \\ if\,(x_{n+1}^{(2)} < -1) \quad then \quad add \quad 2 \\ if\,(x_{n+1}^{(2)} > 1) \quad then \quad substract \quad 2 \end{cases} \tag{21}$$

The results of the modifications are demonstrated on Figs. 13, 14 and 15. The injection mechanism in 3 phases (Fig. 13) pulled regions in an excellent way. The techniques used, greatly improve the points density in the phase space (Figs. 14, 15) where the plotting of 10^9 points are generated. The point distribution of the attractor in phase delay is quite good as well (Fig. 16). Moreover, the largest Lyapunov exponent is equal to *0.5905* indicating a strong chaotic behaviour.
NIST tests are used to verify randomness and system capability to resist main attacks. They require only binary sequences, thus 4×10^6 points were generated, the first 5×10^5 were cut off. The rest of the sequence was converted to

binary form according to the standard IEEE-754 (32 bit single precision floats). Both states of the generator successfully passed NIST tests demonstrating strong randomness being robustness against numerous statistical attacks (Fig. 17). Moreover, we can say that generated sequences look like truly random. Thus, if the adversary looks at the sequence it will be difficult to distinguish it from a truly random generator.

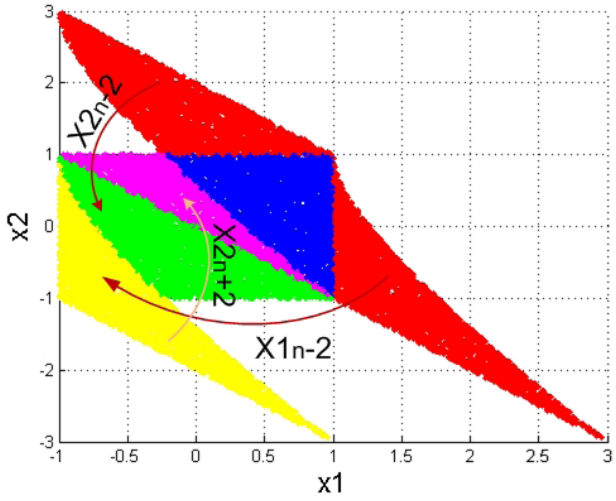


Figure 13: Injection mechanism (21) of $MTTL_2^{SC}$ alternative map

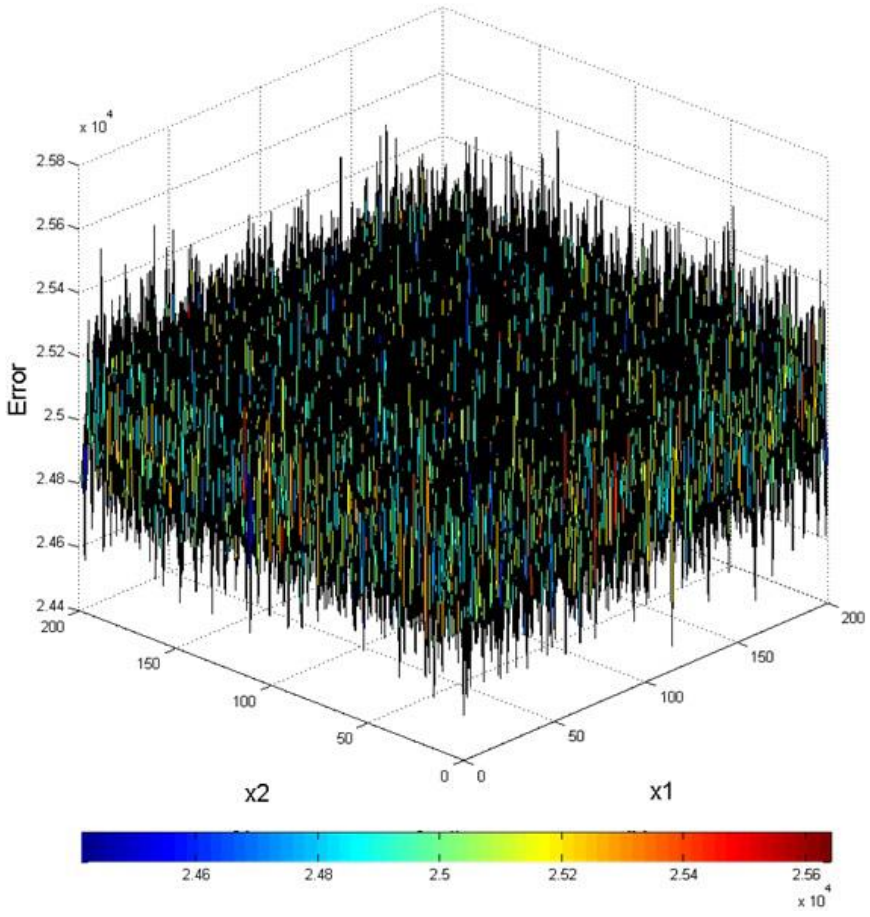
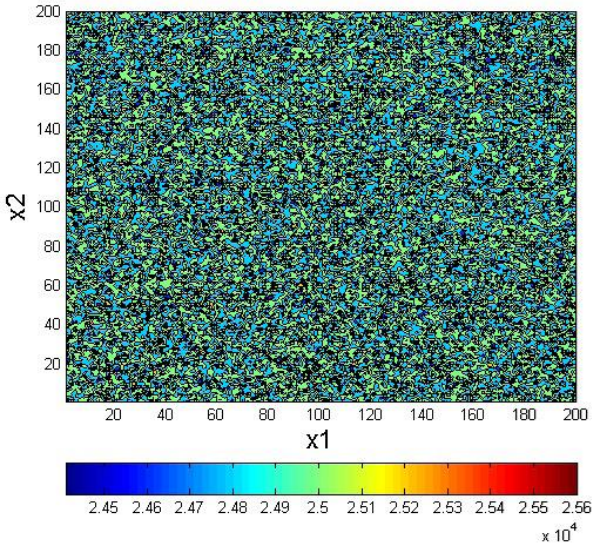


Figure 14: Approximate density function of $MTTL_2^{SC}$ alternative map, which is bounded in a neighbor of 2.5 ± 0.04



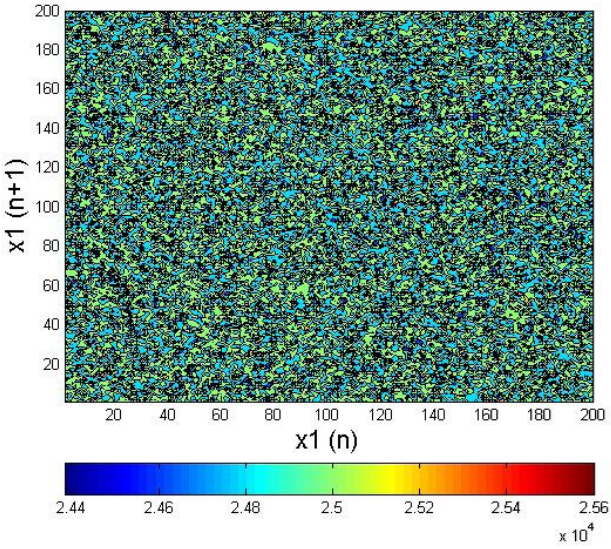


Figure 15 (left): Approximate density function of $MTTL_2^{SC}$ alternative map, on the $(x^{(1)}, x^{(2)})$ plane

Figure 16 (right): Approximate density function of $MTTL_2^{SC}$ alternative map, on the phase delay $(x_n^{(1)}, x_{n+1}^{(1)})$ plane

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/Modified TL_{\mu}^{SC} alternative map_x1.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	8	11	9	10	8	11	15	11	9	0.897763	100/100	Frequency
13	13	12	7	11	10	12	9	5	8	0.678686	99/100	BlockFrequency
6	7	5	12	16	12	12	9	14	7	0.191687	100/100	CumulativeSums
8	10	12	6	14	12	9	6	12	11	0.678686	100/100	Runs
14	11	12	10	15	5	6	13	8	6	0.236810	99/100	LongestRun
9	6	13	10	7	10	11	11	12	11	0.897763	97/100	Rank
11	12	6	19	4	11	11	13	8	5	0.037566	97/100	FFT
7	9	13	14	12	9	9	11	7	9	0.816537	100/100	NonOverlappingTemplate
10	11	15	10	11	9	12	6	11	5	0.595549	98/100	OverlappingTemplate
11	10	5	7	5	13	16	5	13	15	0.058984	100/100	Universal
14	6	11	10	7	9	13	12	8	10	0.739918	98/100	ApproximateEntropy
2	9	7	8	5	7	5	5	8	7	0.689019	63/63	RandomExcursions
5	8	4	4	6	4	4	11	6	11	0.222869	63/63	RandomExcursionsVariant
12	10	12	13	7	8	7	7	6	18	0.171867	99/100	Serial
9	13	11	12	7	9	7	16	7	9	0.534146	99/100	LinearComplexity

(a)

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/Modified TL_{\mu}^{SC} alternative map_x2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
18	6	8	12	9	6	7	10	11	13	0.191687	98/100	Frequency
12	7	12	7	3	11	13	10	13	12	0.366918	98/100	BlockFrequency
15	14	8	6	8	13	7	10	9	10	0.494392	98/100	CumulativeSums
12	15	11	8	7	12	9	5	8	13	0.474986	98/100	Runs
9	12	13	13	9	14	9	6	8	7	0.637119	100/100	LongestRun
8	12	8	10	13	15	10	6	7	11	0.616305	98/100	Rank
8	12	9	15	9	8	17	9	9	4	0.181557	99/100	FFT
7	12	7	12	6	9	15	12	7	13	0.437274	100/100	NonOverlappingTemplate
9	12	11	3	16	8	10	13	10	8	0.289667	99/100	OverlappingTemplate
9	13	10	6	8	8	11	10	11	14	0.816537	99/100	Universal
7	24	9	7	7	8	8	17	7	6	0.000347	98/100	ApproximateEntropy
2	4	2	5	5	7	2	13	4	8	0.011791	52/52	RandomExcursions
5	4	8	5	2	1	8	6	4	9	0.191687	52/52	RandomExcursionsVariant
6	10	8	7	15	15	15	8	8	8	0.236810	100/100	Serial
7	9	11	11	6	15	7	11	8	15	0.419021	99/100	LinearComplexity

(b)

Figure 17: $MTTL_2^{SC}$ alternative map successfully passed NIST tests (a) $x^{(1)}$, (b) $x^{(1)}$

4 A new higher-dimensional map

Higher dimensional systems allow achieving the best randomness, chaoticity and point distribution, because there are more perturbations and nonlinear mixing in it. Usually, 3 or more dimensions are enough to create robust random sequences. Thus, it is an advantage if the system could increase its dimensions. Since, $MTTL_2^{SC}$ alternative map cannot be nested in higher dimension, we describe how to improve randomness, best points distribution and more complex dynamics than $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map.

The best way to achieve randomness from chaos is to couple states with auto and ring-coupling [23]. After applying the conditions the higher dimension map takes form as follow:

$$TTL_2^{RC} = \begin{cases} x_{n+1}^{(1)} = 1 - 2\left|x_n^{(1)}\right| + 2\left(\left|x_n^{(2)}\right| - (x_n^{(1)})^2\right) \\ x_{n+1}^{(2)} = 1 - 2\left|x_n^{(2)}\right| + 2\left(\left|x_n^{(3)}\right| - (x_n^{(2)})^2\right) \\ \vdots \\ x_{n+1}^{(p)} = 1 - 2\left|x_n^{(p)}\right| + 2\left(\left|x_n^{(1)}\right| - (x_n^{(p)})^2\right) \end{cases} \tag{22}$$

The injection is applied as well by verifying each of the state for diverging, in the case if, the injection is used.
Note, each of the states has to satisfy requirements and chaoticity. Therefore, the 3-D and 4-D system were studied for criteria 1-8 (Fig. 4) independently for the each states and in correlation between them. All of the tests have been successfully passed with improving results whereas dimension is higher. Here we demonstrate only more significant and important tests.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	14	8	9	10	9	11	12	6	13	0.779188	100/100	Frequency
11	9	9	8	6	15	7	13	9	13	0.574903	100/100	BlockFrequency
14	6	13	7	11	5	10	11	9	14	0.401199	100/100	CumulativeSums
12	10	7	7	16	8	13	7	13	7	0.366918	99/100	CumulativeSums
16	9	7	11	14	12	6	13	7	5	0.181557	100/100	Runs
13	9	14	11	11	8	9	12	5	8	0.678686	100/100	LongestRun
14	9	7	8	9	16	9	12	6	10	0.455937	100/100	Rank
13	4	9	11	7	4	10	12	19	11	0.037566	100/100	FFT
14	8	8	9	8	15	11	11	8	8	0.699313	100/100	NonOverlappingTemplate
14	15	12	10	6	9	13	7	3	11	0.162606	99/100	OverlappingTemplate
8	7	11	16	9	12	10	9	7	11	0.678686	100/100	Universal
13	11	10	12	6	12	12	14	6	4	0.304126	97/100	ApproximateEntropy
5	5	6	9	2	7	5	8	9	6	0.637119	62/62	RandomExcursions
6	2	4	9	6	11	6	5	6	7	0.407091	62/62	RandomExcursionsVariant
13	8	15	8	12	9	7	15	8	5	0.275709	99/100	Serial
13	6	15	12	11	6	15	8	8	6	0.213309	99/100	Serial
9	6	8	13	8	11	10	11	12	12	0.883171	99/100	LinearComplexity

(a)

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	5	12	14	10	9	12	16	8	7	0.289667	99/100	Frequency
7	7	9	10	6	10	14	8	10	19	0.137282	99/100	BlockFrequency
8	2	9	16	13	9	13	9	7	14	0.090936	99/100	CumulativeSums
5	8	14	11	11	11	14	5	10	11	0.437274	99/100	CumulativeSums
6	16	13	11	9	10	8	7	11	9	0.554420	100/100	Runs
9	13	6	9	14	10	8	11	12	8	0.779188	99/100	LongestRun
9	8	14	6	12	12	8	10	8	13	0.719747	100/100	Rank
10	10	17	5	9	13	14	10	6	6	0.153763	99/100	FFT
9	7	9	13	9	10	10	14	6	13	0.719747	100/100	NonOverlappingTemplate
5	9	12	7	7	12	12	13	12	11	0.637119	99/100	OverlappingTemplate
12	16	8	7	9	10	7	12	8	11	0.616305	99/100	Universal
8	16	6	12	11	13	5	7	13	9	0.249284	99/100	ApproximateEntropy
4	8	4	6	8	5	7	8	9	7	0.804337	66/66	RandomExcursions
4	7	7	8	2	8	6	8	7	9	0.602458	66/66	RandomExcursionsVariant
11	10	10	18	6	5	11	12	10	7	0.213309	100/100	Serial
8	11	10	10	12	11	10	9	9	10	0.998821	98/100	Serial
10	7	13	11	8	7	11	14	11	8	0.798139	99/100	LinearComplexity

(b)

Fig. 1.25 NIST tests for (a) 3-D TTL_2^{RC} alternative map; (b) 4-D TTL_2^{RC} alternative map

Table 1 Numerical results of the error point distribution for 3-D TTL_2^{RC} alternative map

Points	$x^{(i)}x^{(j)}$	$ErrorL1$	$ErrorL2$	$ErrorL3$
10^4	$x^{(1)}x^{(2)}$	1.55695000000012	3.98719999999827	16
10^4	$x^{(1)}x^{(3)}$	1.55960000000011	4.02879999999834	16
10^4	$x^{(2)}x^{(3)}$	1.55850000000012	4.0111999999983	16
10^6	$x^{(1)}x^{(2)}$	0.160244000000057	0.406133599999969	1.56
10^6	$x^{(1)}x^{(3)}$	0.159324000000056	0.400406399999964	1.72
10^6	$x^{(2)}x^{(3)}$	0.159722000000056	0.401812799999966	1.64
10^8	$x^{(1)}x^{(2)}$	0.0175167799999997	0.0483318551999966	0.1788
10^8	$x^{(1)}x^{(3)}$	0.0176578999999997	0.0488421623999967	0.1784
10^8	$x^{(2)}x^{(3)}$	0.0176171399999997	0.0485752623999967	0.1836
10^9	$x^{(1)}x^{(2)}$	0.00908920799999996	0.0125199035839995	0.0772
10^9	$x^{(1)}x^{(3)}$	0.00903516200000002	0.0124306507039994	0.08368
10^9	$x^{(2)}x^{(3)}$	0.00907240999999998	0.0124629701279995	0.07804

Table 2 Numerical results of the error point distribution for 4-D TTL_2^{RC} alternative map

Points	$x^{(i)}x^{(j)}$	$ErrorL1$	$ErrorL2$	$ErrorL3$
10^4	$x^{(1)}x^{(2)}$	1.55720000000011	3.9991999999983	16
10^4	$x^{(1)}x^{(3)}$	1.55655000000012	3.96879999999831	16
10^4	$x^{(1)}x^{(4)}$	1.55495000000012	3.95519999999832	20
10^4	$x^{(2)}x^{(3)}$	1.5581000000001	4.0063999999983	16
10^4	$x^{(2)}x^{(4)}$	1.5576000000001	4.0047999999983	16
10^4	$x^{(3)}x^{(4)}$	1.55395000000012	3.93519999999834	16
10^6	$x^{(1)}x^{(2)}$	0.158570000000055	0.398432799999969	1.64
10^6	$x^{(1)}x^{(3)}$	0.159702000000056	0.404377599999966	1.68
10^6	$x^{(1)}x^{(4)}$	0.160002000000056	0.405107199999971	1.64
10^6	$x^{(2)}x^{(3)}$	0.158936000000056	0.399593599999971	1.52
10^6	$x^{(2)}x^{(4)}$	0.159348000000055	0.401847999999965	1.68
10^6	$x^{(3)}x^{(4)}$	0.158972000000057	0.399148799999965	1.72
10^8	$x^{(1)}x^{(2)}$	0.0159831399999994	0.0400194487999969	0.1608
10^8	$x^{(1)}x^{(3)}$	0.0160255399999995	0.040381923199997	0.1772
10^8	$x^{(1)}x^{(4)}$	0.0160366599999995	0.0404230903999969	0.1852
10^8	$x^{(2)}x^{(3)}$	0.0160441999999995	0.0403678407999969	0.1732
10^8	$x^{(2)}x^{(4)}$	0.0158792799999996	0.0396031839999973	0.1612
10^8	$x^{(3)}x^{(4)}$	0.0158101199999993	0.039183199999997	0.164
10^9	$x^{(1)}x^{(2)}$	0.00507232799999997	0.00404898352000012	0.0524
10^9	$x^{(1)}x^{(3)}$	0.00515058999999998	0.00415637283200005	0.05388
10^9	$x^{(1)}x^{(4)}$	0.00504731199999992	0.00399370235200004	0.05932
10^9	$x^{(2)}x^{(3)}$	0.00505795999999996	0.00400627627200004	0.05516
10^9	$x^{(2)}x^{(4)}$	0.00514836599999991	0.00416637750400014	0.05228
10^9	$x^{(3)}x^{(4)}$	0.00503734799999993	0.00397888753600011	0.05112

5 Conclusion

In this paper we have proposed the original idea to couple two well-known chaotic maps (tent and logistic one), which considered separately - don't exhibit the required features for encryption purposes. However, the new coupling changed qualitatively the overall system behavior, because the maps used with injection mechanism and coupling between states increas their complexity.

We have explored several topologies and finally proposed a new 2-D CPRNG. The proposed model with injection mechanism allows to puzzle perfectly the pieces of the chaotic attractor, like a true random generator. To achieve the best distribution in the phase space, the modified form $MTTL_2^{SC}$ alternative map has been proposed.

The new map exhibits excellent features due to the injection mechanism and enables the uniform density in the state space. The system exhibits strong nonlinear dynamics, demonstrating great sensitivity to initial conditions. It generates an infinite range of intensive chaotic behavior with large positive Lyapunov exponent values. Moreover, $MTTL_2^{SC}$ successfully passed all required tests: cross-correlation, autocorrelation, LLE, NIST tests, uniform attractor on the phase space and phase delay. The system analysis and the dynamics evolution by bifurcation diagram and topological mixing proved the complex behavior. The system orbits exhibited complex behavior with perfect mixing. The study demonstrated totally unpredictable dynamics making the system strong-potential candidate for high-security applications.

Finally, the dimension of the TTL_2^{RC} non-alternative map is easily increased whenever it is necessary to reach the strongest security requirements as shown in Sect. 4.

References

[1] Menezes, A. J. & Van Oorschot, P. C.: *Handbook of applied cryptography*, CRC press (1996).

[2] Li, C.-Y., Chen, Y.-H., Chang, T.-Y., Deng, L.-Y. & Kiwing, T.: Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 20 (2), 385-389 (2012).

[3] Lozi, R. & Cherrier, E.: Noise-resisting ciphering based on a chaotic multi-stream pseudorandom number generator. *In* Proc. 2011 International Conference for Internet Technology and Secured Transactions (ICITST), Abu Dhabi, 91-96 (2011).

[4] Noura, H., El Assad, S., Vladeanu, C.: Design of a fast and robust chaos-based cryptosystem for image encryption. *In* 8th International Conference on Communications (COMM 2010), 423-426 (2010).

[5] Julia, G.: Mémoire sur l'itération des fonctions rationnelles. Journal de mathématiques pures et appliquées, 8ème série, tome 1, 47-246 (1918).

[6] Fatou, P.: Sur l'itération des fonctions transcendantes entières. Acta Math, 47, 337-370 (1926).

[7] Sharkovskiĭ, A. N.: Coexistence of cycles of a continuous map of the line into itself. Ukrainian Math. J.,16 , 61-71 (1964) [in Russian]. International Journal Bifurcation & Chaos, 5 (5), 1263-1273 (1995).

[8] Gumowski, I. & Mira, C.: Recurrence and Discrete Dynamics systems, Lecture Notes in Mathematics, Springer, Berlin, Germany, (1980).

[9] Sprott, J.C.: Can a Monkey with a Computer Create Art? Nonlinear Dynamics, Psychology, and Life Sciences, 8, 103-114 (2004).

[10] Chua, L. O., Kumoro, M. & Matsumoto, T.: The Double Scroll Family. IEEE Trans. Circuit and Systems, 32 (11), 1055-1058, (1984).

[11] Hénon, M.: A Two-dimensional mapping with a strange attractor. Commun. Math. Phys., 50, 69-77 (1976).

[12] Lozi, R.: Mathematical Chaotic circuits: an efficient tool for shaping numerous architectures of mixed Chaotic/pseudo random number generator. *In* Proceedings Mendel 2014, (Ed. M. Matoušek), 163-176 (2014).

[13] Sudret, B.: Global sensitivity analysis using polynomial chaos expansions. Reliability Engineering and System Safety 93, 964-979 (2008)

[14] Lozi, R.: Can we trust in numerical computations of chaotic solutions of dynamical systems?, *Topology and Dynamics of Chaos*, Eds. Ch. Letellier, R. Gilmore, World Scientific Series on Nonlinear Sciences , Series A, 84, 63-98 (2013).

[15] Baptista, M. S.: Cryptography with chaos. Phys. Lett. A, 240, 50-54 (1998).

[16] Ariffin, M. R. K., Noorani, M. S. M.: Modified Baptista type chaotic cryptosystem via matrix secret key. Phys. Lett. A, 372, 5427-5430 (2008).

[17] Garasym, O., Taralova, I. & Lozi, R.: New nonlinear CPRNG based on tent and logistic map (To appear).

[18] Lanford III, O. E: Informal remarks on the orbit structure of discrete approximations to chaotic maps. Experimental Mathematics 7, 317-324 (1998).

[19] Yuan, G. & Yorke, J. A: Collapsing of chaos in one dimensional maps. Physica D: Nonlinear Phenomena 136, 18-30 (2000).

[20] Wong, W. K., Lee, L. P. & Wong, K. W.: A modified chaotic cryptographic method. Communications and Multimedia Security Issues of the New Century, 123-126 (2001).

[21] Nejati, H., Beirami, A., & Massoud, Y.: A realizable modified tent map for true random number generation. Circuits and Systems, MWSCAS 10, 621-624 (2008).

[22] Rojas, A., Taralova, I. & Lozi, R.: New alternate ring-coupled map for multirandom number generation. Journal of Nonlinear Systems and Applications 4 (1), 64-69 (2013).

[23] Lozi, R.: Emergence of randomness from chaos. International Journal of Bifurcation and Chaos, 22 (2), 1250021-1/1250021-15 (2012).